United States Department of Agriculture (USDA)
eGovernment Program

USDA eAuthentication Service
Privacy Impact Assessment

September 22, 2005

Table of Contents

1 Introduction

1.1 eAuthentication Overview

The USDA eAuthentication Service provides single sign-on capability for access to USDA web applications, management of user credentials, and verification of identity. USDA eAuthentication enables secure electronic transactions by providing an electronic identity validation to allow electronic signatures and non-repudiation. Through a self-registration process USDA customers and employees are able to obtain accounts as authorized users that will enable them to access USDA Web applications and services via the Internet.

The eAuthentication Service enables users to securely and confidently conduct business transactions with the USDA electronically via the Internet. It is imperative to provide individuals with a clear understanding of eAuthentication's policies and procedures for ensuring privacy protection of customer and employee information.

1.2 Purpose

This document details a Privacy Impact Assessment (PIA) of the USDA eAuthentication Service. The purpose of this document is the following:

- Provide clear well-defined documentation on how eAuthentication manages customer and employee data.
- Build trust and reliance in eAuthentication's ability to provide secure online transactions and protect user information from unauthorized access.
- Provide awareness on the information that eAuthentication collects and the purpose for what it is used.
- Assure USDA customers and employees that collected information is necessary, and is used to perform the system's designed functions.
- Discuss the security controls used by eAuthentication to protect user information and discuss how the system mitigates privacy risks.

2 Privacy Impact Assessment

2.1 Purpose and Use of Collected Information

The eAuthentication Service collects customer and employee information for the purpose of creating eAuthentication accounts that are used to authenticate users to USDA Web applications. In addition, customer and employee account information is provided to USDA applications which the user chooses to access, in order to facilitate authorization and business transactions.

2.2 Authority to Collect Information

The USDA eAuthentication Service derives the authority to collect user information from the following statutes and regulations:

E-Government Act of 2002 (H.R. 2458)

This legislation ensures strong leadership of information technology activities of Federal agencies, a comprehensive framework for information security standards and programs, and uniform safeguards to protect the confidentiality of information provided by the public.

Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998

The Government Paperwork Elimination Act (GPEA) required agencies, by October 21, 2003, to provide an electronic option for maintenance, submission, or disclosure of information, when practicable as a substitute for paper. GPEA also entails the use and acceptance of electronic signatures, when practicable.

Freedom to E-File Act (Pub. L. 106-222) of 2000

To the maximum extent practicable, this act establishes an Internet-based system that enables agricultural producers to access all forms of the agencies of the Department of Agriculture.

Electronic Signatures in Global and National Commerce Act (E-SIGN, Pub. L. 106-229) of 2000

The E-SIGN Act recognizes the validity of contracts in electronic form. It not only authorizes digital signatures, which enables electronic authentication, but also empowers the use of online contracting and provision of notices.

USDA eAuthentication operates under the aforementioned regulations and collects information solely to accomplish its designed purpose as noted in the regulations. The

authority to collect information is approved by the Office of Management and Budget (OMB) under OMB Control Number 0503-0014. Furnishing the requested information is voluntary. However, if this information is not provided, electronic access to USDA Web applications that are protected by eAuthentication will not be permitted.

2.3 Information Collection

The USDA eAuthentication Service collects user information in order to provide authorized user accounts that facilitate access to USDA resources protected by eAuthentication.

The eAuthentication Web site does not collect information that is considered of a sensitive nature such as race, religious beliefs, and sexual behavior and attitude. In addition to the identity information collected at registration and described in sections 2.3.1 and 2.3.2, each eAuthentication account also contains an associated user ID and password that was created by the user. In addition, each account may contain associated roles or permissions, given by specific USDA administrators, which allow the user to access certain requested applications. The user ID and password and permissions associated with an account are what enable users to access requested USDA resources.

For more information on the procedures for applying for an eAuthentication account please review the eAuthentication *Customer Registration Job Aid* document. This document is included in the eAuthentication Information Collection Package.

2.3.1 USDA Customers

User accounts are obtained through a voluntary self-registration process provided by the eAuthentication Web site, located at www.eauth.egov.usda.gov. USDA customers can self-register for a Level 1 or Level 2 Access account. A Level 1 Access account provides users with limited access to USDA Web site portals and applications that have minimal security requirements. A Level 2 Access account enables users to conduct official electronic business transactions via the Internet, enter into a contract with USDA, and submit forms electronically via the Internet to USDA Agencies. Due to the increased customer access associated with a Level 2 Access account, customers must be authenticated in person at a USDA Service Center by a Local Registration Authority (LRA), in addition to an electronic self-registration. This provides a level of assurance in the customer's identity that is not present through the self-registration.

The following information is collected from customers through the electronic self-registration process:

Level 1 Access ***Required*** User ID Password	**Level 2 Access** ***Required*** User ID Password

Email Address First Name Last Name Country Name ***Optional*** Middle Initial Home Postal/ZIP Code	Email Address First Name Last Name Address City State Home Postal/ZIP Code Country Name Mother's Maiden Name 4 digit PIN Date of Birth ***Optional*** Middle Initial Home Phone International Home Phone Alternate Phone International Alternate Phone SCIMS Account Number

During the in-person identity proofing process for Level 2 accounts, the credential document type and expiration date is also recorded. At this time, the SCIMS account number may be also entered into the record by the Local Registration Authority, if the customer has had previous business with the USDA Service Center Agencies. Information about the SCIMS system can be found at http://www.fsa.usda.gov/dam/kcmo/itsd/scit_projects.htm.

	Identity-Proofing Information Name of LRA Credential Document Type Credential Expiration Date

2.3.2 USDA Employees

The USDA employee self-registration process provides a Level 2 Access account electronically. Identity confirmation is accomplished by verifying inputted information against employee data from the Common Employee Database (CED). This database includes information found on earnings and leave statements created by the National Finance Center. This online registration process also provides a level of assurance in the employee's identity, without the in-person identity-proofing required of customers.

The following information is collected from employees through the electronic self-registration process:

Employee Account

Required
- User ID
- Password
- Email Address
- First Name
- Last Name
- Address
- City
- State
- Home Postal/ZIP Code
- Country Name
- Mother's Maiden Name
- 4 digit PIN
- Date of Birth
- Agency Name
- Social Security Number
- Duty Station Code
- Service Comp. Date
- Net Amount of Paycheck
- Pay Plan, Grade, and Step

Optional
- Middle Initial
- Home Phone
- International Home Phone
- Alternate Phone
- International Alternate Phone

2.4 Information Sources

2.4.1 USDA Customers

The eAuthentication Service collects information from any individual requesting access to USDA online resources that are protected by eAuthentication. The information is collected through a one-time electronic self-registration form provided through the eAuthentication website, located at www.eauth.egov.usda.gov. This enables customers and employees to register for an eAuthentication account that will provide access to protected USDA Web applications and services.

Identity-proofing information is collected by the Local Registration Authority (LRA). During the time of in-person identity-proofing the LRA must record the credential document type and expiration date. In addition, the SCIMS account number may be also entered into the record by the Local Registration Authority, if the customer has had previous business with the USDA Service Center Agencies. Information about the SCIMS system can be found at http://www.fsa.usda.gov/dam/kcmo/itsd/scit_projects.htm.

2.4.2 USDA Employees

In addition to the self-registration process, the eAuthentication System also obtains data from the USDA Common Employee Database (CED) to validate entered employee information. eAuthentication verifies the identity of employees during the registration process by comparing the entered information against data in CED. This allows employees to register without the in-person identity-proofing required of customers. More information about CED is available through Departmental Regulation 3630-001.

2.5 Data Attributes

2.5.1 Necessity

The USDA eAuthentication Service collects customer and employee information in order to provide a level of assurance of the identity of the user, prior to allowing access to USDA Web resources. Information is collected for 2 reasons:

- to initially validate the user's identity
- to verify that the returning user is the same identity-proofed customer or employee (via the user ID and password)

2.5.2 Completeness

Customers and employees must register through an online self-registration process in order to obtain an eAuthentication account. The online self-registration forms contain required and optional fields for users to enter their personal information. Completeness of data is ensured by requiring users to complete all required fields prior to submission. The eAuthentication Service prohibits users from submitting their registration without the required minimum user information.

2.5.3 Accuracy

The online self-registration forms include automatic format validation of some entered user data. Customers and employees are prohibited from submitting registration forms unless all required data fields are completed in a valid format. In addition, form data requires users to enter their password twice and uses dropdown lists for predictable fields such as state and country. These controls ensure that user data is accurately collected in a proper format.

In addition, for a Level 2 Access account, customers are required to travel to a USDA Service Center to validate their registration data against a government ID.

Customer and employee information is kept current by allowing users to electronically update their own basic personal information such as address and email. Once a user submits their modified information, the system is immediately updated to reflect these changes.

2.6 Information Sharing

2.6.1 USDA Applications

The USDA eAuthentication Service provides Site Protection to USDA Web applications. As part of this function, eAuthentication discloses user identity and credential information, such as level of assurance, to the requested application to enable user access. The eAuthentication Service shares this data upon initial access to the Web application. Target application owners are then responsible for securing the data within their application.

2.6.2 Federal Government E-Authentication

The eAuthentication Service also serves as a Credential Service Provider in the government's federated architecture. In this capacity, eAuthentication discloses user credential information to external applications that are also integrated with the government's federated architecture if the user has chosen to access these applications.

All applications must have completed a Certification and Accreditation (C&A), as well as the GSA boarding process, in order to join the Federation. The GSA boarding process requires agencies to be compliant with the Paperwork Reduction Act and complete a System of Records Notice. GSA also requires agencies to meet architecture/technical interface requirements to ensure a secure and effective technical environment.

2.6.3 Data Sharing Requirements

Additional data passed to any system must meet the following conditions:

- System owner must provide a written request and justification as to why the data elements eAuthentication are required.
- Target system has an approved and valid Certification and Accreditation (C&A) Authority to Operate (ATO) in effect.
- If shared data comprises of identifiable user information, the target system must have a current Privacy Impact Assessment (PIA) on file with the USDA Information Officer.
- System owner must sign a Memorandum of Understanding (MOU) with eAuthentication agreeing that they will use the information only as stipulated in the request, will not transfer received data to other external parties, and will maintain sufficient security as stipulated in their C&A Security Test and Evaluation (ST&E).

2.6.4 Data Attributes Sharing Policy

The eAuthentication Service does not share sensitive data attributes such as user ID, password, or account security attributes under any circumstances. Confidential data such

as name, address, and contact information is conditionally shared. Internal data such as organization information for employees is also conditionally shared.

The USDA eAuthentication Service will also disclose personal information to government entities for law compliance purposes. A complete description of these information uses is described in Section 3.3: Privacy Act System of Records in the Appendix.

2.7 Access to System Data

The USDA eAuthentication Service is responsible for protecting the privacy rights of customers and employees who provide their personal information. Access to system data is granted on a limited basis to USDA customers, employees, administrators, help desk individuals, and other federal agencies to facilitate electronic user authentication and authorization.

USDA customers and employees are granted access to their own basic personal information. Users can use their account's user ID and password to access and modify basic personal data such as address and email. Users do not have access to modify sensitive data such as level of access and permissions associated with an account. Only system administrators have access to update sensitive fields, and only do so when a ticket is escalated from the help desk.

System administrators have access to user information on a limited basis allowing them to only perform their specific job function. Access is limited to administrators on a least privileged basis utilizing separation of duties. Administrators and help desk persons have eAuthentication accounts with the appropriate level of access and permissions which allow them to access and modify user data. These permissions are granted by a limited number of management personnel.

The eAuthentication system contains effective reporting capabilities to report access to system data. eAuthentication is able to report account creation and data modification facts. For account credentials, eAuthentication is able to report the date, time, and individual responsible for granted permissions and increased level of access.

2.8 System Security

The USDA eAuthentication Service has conducted a comprehensive and thorough Certification and Accreditation (C&A) and is fully authorized to operate. The eAuthentication Service is accredited and formally declared to have implemented appropriate security controls and have a satisfactory level of security present in the system.

Furthermore, the eAuthentication Service is fully compliant with the Federal Information Security Management Act (FISMA) of 2002 and meets or exceeds standard security

controls set forth by the National Institute of Standards and Technology (NIST). These regulations require all federal agencies to provide security for the information and information systems that support the operations and assets of the agency. In addition, the following security controls are utilized and continuously reviewed to ensure a high level of security control for the eAuthentication system.

- Vulnerability Assessments
- Host-Based Intrusion Detection
- Network-Based Intrusion Detection
- Firewall Alerting
- USDA Intrusion Detection
- Active Directory Monitoring
- Database Monitoring
- Site Protection Monitoring
- Identity Management Monitoring
- Virus Protection
- Machine Health

All systems interacting with eAuthentication are required to have appropriate security controls. This includes the hosting facility, Web Farm, and integrated applications. Integrated target systems must have a valid C&A ATO in effect and memorandum of understanding to ensure that information is only used in the intended manner. Please refer to Section 2.7: Information Sharing of this document for more information on the security precautions that are taken before a target system integrates with the eAuthentication solution.

2.9 Data Storage, Retention, and Disposal

Information obtained by the eAuthentication Service is stored and maintained electronically on secure USDA-owned and operated systems in St. Louis, MO, and Ft. Collins, CO. The eAuthentication system, including the data repositories, is replicated between the two locations to ensure consistency. These systems are formally declared to have implemented appropriate security controls and have a valid C&A ATO in effect.

The USDA eAuthentication Service is responsible for maintaining a record of the facts of registration for a period beyond expiration or revocation of a user's credential. Departmental regulation requires eAuthentication to retain user data for a minimum time period. This minimum time period varies with the assurance level of the credential as follows:

- Level 1 credentials – no minimum retention period.
- Level 2 and 3 credentials – seven years and six months.

eAuthentication also maintains records of user registrations, user logons, and account data (data entered, modified, or deleted) through the eAuthentication system. Departmental regulation requires eAuthentication to retain these database auditing logs for a minimum of 7 years. Currently, eAuthentication account records are maintained

indefinitely. Agencies are responsible for maintaining records of application access and data transactions conducted through their applications.

Backups of critical eAuthentication files are taken daily while full server backups are performed on a weekly basis. These critical file backups and server backups are used for a variety of functions from restoring a single audit file that was accidentally deleted to recovering from a hard disk crash. Data, files, directories, and logs are readily available for restore in case of an emergency.

Non-scheduled backups are performed under the following circumstances:

- Before a major software or application installation.
- Before a major hardware installation, transfer, move, or upgrade.
- At the request of the data owner.

Backups are stored on tapes with recognized barcode labels so that in the event of a disaster they are easily identified. They are securely stored in a locked storage cabinet in a different computer room from where the servers are located to prevent losing both the server and the backups in an emergency.

2.10 Privacy Notice

The USDA eAuthentication Service notifies users of privacy information through the following:

- Privacy Act and Public Burden Statements
- Privacy Act System of Records Notice
- Information Collection Notice and Package

The USDA eAuthentication Service notifies customers and employees of the purpose and authority to collect their information through the eAuthentication Privacy Act Statement and Public Burden Statement. The Privacy Act Statement informs users of the authority by which information is collected, purpose and use of the collected information, and repercussions for not providing the information. The Public Burden Statement informs users of the OMB control number by which eAuthentication collects information and provides estimates on the time required to complete the registration process. The OMB control number is also listed on all customer registration forms. Users can view the Privacy Act and Public Burden Statements on the Privacy Policy page of the eAuthentication Web site. Copies of these statements are included in Section 3.2: Privacy Act and Public Burden Statements in the Appendix.

The USDA eAuthentication Service also notifies customers and employees of system properties and the collection and management of user data through the USDA eAuthentication Service System of Records, which is published in the federal register.

The Information Collection Package provides a detailed description of the eAuthentication information collection process. The information collection notice is also published in the federal register. Copies of these documents are included in Section 3.3: Privacy Act System of Records and Section 3.4: Information Collection Supporting Statement in the Appendix.

3 Appendix: Supporting Documents

3.1 Privacy Impact Assessment Questionnaire

Introduction

This document reports the results of a Privacy Impact Assessment conducted on the USDA eAuthentication Service in July 2005. The assessment was conducted according to the guidelines set forth in *Cyber Security Guidance on Privacy Impact Assessments (PIAs)*, and presents the information requested in Attachment 2, USDA Privacy Impact Assessment Form.

Assessment Results

Project Name: USDA eAuthentication Service

Program/Project Description:

The USDA eAuthentication Service provides USDA Agency customers and employees single sign-on capability and electronic authentication and authorization for USDA Web applications and services. Through an online self-registration process, USDA Agency customers and employees can obtain accounts as authorized users that will provide access to USDA resources without needing to reauthenticate within the context of a single internet session. Once an account is activated, users may use the associated user ID and password that they created to access USDA resources that are protected by eAuthentication.

DATA IN THE SYSTEM

1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	**Webusers** Level 1: User ID* Password* First Name* Middle Initial Last Name* Home Postal/Zip Code Country name* Email* EAuth Internal ID Level of Assurance Level 2: SCIMS ID User ID* Password* First Name* Middle Initial Last Name* Home Address* City* State* Home Postal/Zip Code* Country name* Email* Home Phone International Home Phone Alternate Phone International Alternate Phone Mother's Maiden Name* 4 digit PIN* Date of Birth (DOB) EAuth Internal ID Level of Assurance Identity Proof Type Credential Issuer Credential Document Type Credential Expiration **Employees** eAuthentication AD: FIPS State County Code CAMS Employee ID EAuth Internal ID User ID* Password* Home Address* Home Postal/Zip Code* Home Phone International Home Phone Alternate Phone International Alternate Phone Country name* E-mail* Mother's Maiden Name* 4 digit PIN* Date of Birth (DOB)* Agency Name* First Name* Middle Initial Last Name* State* City* Level of Assurance* Common Employee Database: Social Security Number (SSN) Duty Station Code* Service Comp. Date* Net Amount of Paycheck* Pay Plan, Grade, and Step* (*) Required information

2a. What are the sources of the information in the system?	1) Individuals registering for accounts 2) USDA Common Employee Database 3) USDA Service Center Information Management System (SCIMS) database.
2b. What USDA files and databases are used? What is the source agency?	Common Employee Database (CED) – USDA OCIO
2c. What Federal Agencies are providing data for use in the system?	1) The United States Department of Agriculture 2) In the long term, USDA will accept data from other Federal Agencies that are certified as credential providers by General Services Administration (GSA) as part of the E-Authentication initiative.
2d. What State and Local Agencies are providing data for use in the system?	No state or local agency is providing data for use in the system.
2e. From what other third party sources will data be collected?	Data will not be collected from other third party sources.

2f. What information will be collected from the customer/employee?	**Webusers** Level 1: User ID* Password* First Name* Middle Initial Last Name* Home Postal/Zip Code Country name* Email* Level 2: User ID* Password* First Name* Middle Initial Last Name* Home Address* City* State* Home Postal/Zip Code* Country name* Email* Home Phone International Home Phone Alternate Phone International Alternate Phone Mother's Maiden Name* 4 digit PIN* Date of Birth (DOB)* **Employees** UserName Password Home Address Home Postal/Zip Code Home Phone International Home Phone Alternate Phone International Alternate Phone Country name Email Social Security Number (SSN) Mother's Maiden Name* 4 digit PIN* Date of Birth (DOB)* Agency Name* Duty Station Code* Service Comp. Date* First Name* Middle Initial Last Name* State* City* Net Amount of Paycheck* Pay Plan, Grade, and Step* * Required information
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	All information is provided by the customer or from USDA records.

3b. How will data be checked for completeness?	Customer information is self-service entered. For Level 2 Access accounts, customer information is validated by a Local Registration Authority (LRA). The LRA checks the information in the USDA eAuthentication Service against the customer's identification. Employee information is validated against USDA payroll and personnel information from a common employee database. Self-registration includes validations such as entry of required fields, confirming passwords by entering it twice and using dropdown lists for "state" and other predictable fields. A registration form cannot be submitted unless all required fields are entered correctly.

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	Users have limited access to their own data. System Administrators, database administrators, and help desk persons have access to data fields on a least privileged basis.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	End users have access only to their own information and have write privileges to a very limited subset of this information. System administrators, database administrators and help desk persons have access based on criteria limiting access to only that needed for the individuals to do their specified job. Controls have been established for access management and are documented in the system's Certification and Accreditation.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	End users have access only to their own information and have write privileges to a very limited subset of this information. System administrators, database administrators and help desk persons have access based on criteria limiting access to only that needed for the individuals to do their specified job. Controls have been established for access management and are documented in the system's Certification and Accreditation.

4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	Access is limited to system administrators, data base administrators, and help desk users on a least privilege basis utilizing separation of duties.
5a. Do other systems share data or have access to data in this system? If yes, explain.	eAuthentication provides a standard set of user information to integrated applications in order that authentication and authorization can occur. Only certain data is shared with applications according to our data sharing policy.
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	The USDA eAuthentication Service shares data with applications upon initial authorization. Application owners are then responsible for securing information within their application.
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	In the long term, USDA will accept data and transfer data to other Federal Agencies that are part of the E-Authentication Federation initiative.
6b. How will the data be used by the agency?	The data is used by agency applications to make authentication and authorization decisions and to facilitate business transactions.
6c. Who is responsible for assuring proper use of the data?	The USDA eAuthentication shares data with applications upon initial authorization. Application owners are then responsible for securing information within their application.

ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes, the system was designed as a security front-end to provide authentication and authorization to web-based applications. The data stored within the USDA eAuthentication Service is used to determine authentication and application access.
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	The eAuthentication Service relies upon existing data sources and information collected directly from the customer or employee. The system itself does not derive or create new data.
2b. Will the new data be placed in the individual's record (customer or employee)?	Not Applicable.
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	Not Applicable.
2d. How will the new data be verified for relevance and accuracy?	Not Applicable.

3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	Customer data is not consolidated. Employee data is consolidated in the Common Employee Database (CED). CED is a component of USDA Enterprise Shared Services (ESS). More information about CED is available through Departmental Regulation 3630-001.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	Processes are not consolidated.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Data is retrieved to make authentication and authorization decisions by the eAuthentication Service once a user (employee or customer) enters their ID/Password.
4b. What are the potential effects on the due process rights of customers and employees of: • **consolidation and linkage of files and systems** • **derivation of data** • **accelerated information processing and decision making** • **use of new technologies**	Not Applicable.
4c. How are the effects to be mitigated?	Not Applicable.

MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	The USDA eAuthentication Service centralizes the authentication and authorization process for Web-based applications. Access control is centrally managed ensuring equitable treatment for all employees and customers using Web-based applications protected by the USDA eAuthentication Service.
2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?	The eAuthentication Service is operated in two sites (Fort Collins, Colorado and St. Louis, Missouri). The system including the data repositories are replicated between the cities to ensure consistency.
2b. Explain any possibility of disparate treatment of individuals or groups.	All customers are required to follow the same registration and identity-proofing process. All USDA employees are required to follow the same registration and online identity-proofing process.

2c. What are the retention periods of data in this system?	Data is retained within the USDA eAuthentication Service for a period of • Level 1 credentials – no minimum retention period, • Levels 2 and 3 credentials – minimum of seven years and six months, after the termination of the record as per the USDA disposition authority.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	The procedures have not been created as of this point in time since the USDA eAuthentication Service is only 2 years old.
2e. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	Certain data is refreshed from its sources periodically and other data is maintained by the user. The source applications are responsible for maintaining current and complete data.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	The system is not using technologies in ways that the USDA has not previously employed.
3b. How does the use of this technology affect customer/employee privacy?	Authorized data is shared within USDA.
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	eAuthentication does not locate or monitor individuals.
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	eAuthentication does not identify, locate, or monitor groups of people.
4c. What controls will be used to prevent unauthorized monitoring?	Not Applicable.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	The USDA eAuthentication Service System of Records is in progress. The number is yet to be assigned.
5b. If the system is being modified, will the Systems of Record (SOR) require amendment or revision? Explain.	The new System of Records, which is in progress, is up to date.

3.2 Privacy Act and Public Burden Statements

The following statements notify users of the purpose and use of collected information and provide an estimate of the time burden associated with obtaining an eAuthentication account. The statements are provided to users online in the Privacy Policy page of the eAuthentication Web site, located at www.eauth.egov.usda.gov.

Privacy Act Statement

The following statement is made in accordance with the Privacy Act of 1974 (5 USC 552a) as amended. The authority for requesting the following information is the Government Paperwork Elimination Act, GPEA (Pub. L. 105-277), the Freedom to E-File Act (Pub. L. 106-222), the Electronic Signatures in Global and National Commerce Act, E-SIGN (Pub. L. 106-229), and the E-Government Act of 2002 (H.R. 2458). The information will be used to establish secure information transactions by enabling the electronic authentication and authorization of users desiring access to USDA Web applications and services via the Internet. Furnishing the requested information is voluntary. However, if this information is not provided, electronic access to USDA Web applications and services will not be permitted. This information may be provided to other agencies, IRS, Department of Justice, or other State and Federal Law enforcement agencies, and in response to a court magistrate or administrative tribunal. The provisions of criminal and civil fraud statutes, including 18 USC 286, 287, 371, 641, 651, 1001; 15 USC 714m; and 31 USC 3729, may be applicable to the information provided.

Public Burden Statement

According to the Paperwork Reduction Act of 1995, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0560-0219. The time required to complete this information collection is estimated to average 8 minutes per response for an eAuthentication Level 1 Access account and 1.17 hours per response for an eAuthentication Level 2 Access account, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

3.3 Privacy Act System of Records

USDA eAuthentication Service System of Records

System Name:
USDA eAuthentication Service

Security Classification:
None

System Location:
USDA-NRCS Information Technology Center, 2150 Centre Avenue Building A, Fort Collins, CO 80526-1891; USDA-Rural Development, 1520 Market Street, St. Louis, MO 63103

Categories of Individuals Covered by the System:
This system contains records and related correspondence on individuals who can access USDA applications and services that are protected by eAuthentication. This includes members of the public and USDA employees.

Categories of Records in the System:
The eAuthentication system will collect the following information from individuals when transacting electronically with USDA: name, address, country of residence, telephone, email address, date of birth, and mother's maiden name. The system will also require users to create a user ID and password.

Authority for Maintenance on the System:
Government Paperwork Elimination Act (GPEA, Pub. L. 105-277) of 1998; Freedom to E-File Act (Pub. L. 106-222) of 2000; Electronic Signatures in Global and National Commerce Act (E-SIGN, Pub. L. 106-229) of 2000; eGovernment Act of 2002 (H.R. 2458).

Purpose(s):
The records in this system are used to electronically authenticate and authorize users accessing protected USDA applications and services.

Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses:

1. Disclosure to USDA applications protected by eAuthentication, as a user requests access to individual applications.
2. Disclosure to external web applications integrated with the government's federated architecture for authentication. Under this architecture, the user will request access to an external application with their USDA credential prior to any disclosure of information. All external applications will have undergone rigorous testing before joining the architecture.

3. Referral to the appropriate agency, whether Federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting violation of law, or of enforcing or implementing a statute, rule, regulation, or order issued pursuant thereto, of any record within this system when information available indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature.
4. Disclosure to a court, magistrate, or administrative tribunal, or to opposing counsel in a proceeding before a court, magistrate, or administrative tribunal, of any record within the system that constitutes evidence in that proceeding, or which is sought in the course of discovery, to the extent that USDA determines that the records sought are relevant to the proceeding.
5. Disclosure to a congressional office from the record of an individual in response to any inquiry from the congressional office made at the request of that individual.
6. Disclosure at the individuals' request to any federal department, state or local agencies, or USDA partner utilizing or interfacing with eAuthentication to provide electronic authentication for electronic transactions. The disclosure of this information is required to securely provide, monitor, and analyze the requested program, service, registration, or other transaction.
7. Disclosure to USDA employees or contractors, partner agency employees or contractors, or private industry employed to identify patterns, trends, and anomalies indicative of fraud, waste, or abuse.
8. Disclosure to determine compliance with program requirements.

Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System:

Storage:

Records are stored and maintained electronically on USDA owned and operated systems in St. Louis, MO, and Ft. Collins, CO.

Retrievably:

Records can be retrieved by name, username, or system ID.

Safeguards:

Records are accessible only to authorized personnel. Protection of the records is ensured by appropriate technical controls. The physical security of the system is provided by restricted building access. In addition, increased security is provided by encryption of data when transmitted. The system has undergone a Certification and Accreditation.

Retention and Disposal:

Since records are maintained electronically, they will be retained indefinitely.

System Manager and Address:

Owen Unangst, NRCS Information Technology Center, 2150 Centre Avenue Building A, Fort Collins, CO 80526-1891.

Notification Procedure:

An individual may request information regarding this system of records or information as to whether the system contains records pertaining to such individual from the Ft. Collins office. The request for information should contain the individual's name, username, address, and email address. Before information of any record is released, the system manager may require the individual to provide proof of identity or require the requester to furnish authorization from the individual to permit release of information.

Record Access Procedures:

An individual may obtain information as to the procedures for gaining access to a record in the system, which pertains to such individual, by submitting a request to the Privacy Act Officer, 1400 Independence Avenue SW, South Building, Washington, DC 20250-3700. The envelope and letters should be marked "Privacy Act Request." A request for information should contain name, address, username, name of system of records, year of records in question, and any other pertinent information to help identify the file.

Contesting Record Procedures:

Procedures for contesting records are the same as procedures for record access. Include the reason for contesting the record and the proposed amendment to the information with supporting documentation to show how the record is inaccurate.

Record Source Categories:

Information from the system will be submitted by the user. When a user wishes to transact with USDA or its partner organizations electronically, the user must enter name, address, country of residence, telephone, date of birth, mother's maiden name, username, and password. As the USDA eAuthentication Service is integrated with other government or private sector authentication systems, data may be obtained from those systems to facilitate single-sign on capabilities.

Exemptions Claimed for this System:

None.

3.4 Information Collection Supporting Statement

The following is the Supporting Statement from the eAuthentication Information Collection Package created in July 2005 in compliance with the Paperwork Reduction Act of 1995.

Justification

1. Explain the circumstances that make the collection of information necessary.

The Freedom to E-File Act, Government Paperwork Elimination Act, and the President's Management Agenda prescribe eGovernment functions as alternatives to traditional paper-based processes. Conducting online transactions necessitates processes for authenticating and authorizing online users and completing transactions with an electronic equivalent to traditional ink signatures. The information collected from the eAuthentication Web site enables the electronic authentication and authorization of users to USDA Web-based applications.

2. Indicate how, by whom, how frequently, and for what purpose the information is to be used.

The USDA eAuthentication Service provides public and government businesses single sign-on capability for USDA applications, management of user credentials, and verification of identity, authorization, and electronic signatures. USDA eAuthentication obtains customer information through an electronic self-registration process provided through the eAuthentication Web site. This voluntary online self-registration process applies to USDA Agency customers, as well as employees, who request access to protected USDA Web applications and services via the Internet. Registrants are able to self-register online from the eAuthentication Web site, located at www.eauth.egov.usda.gov, for a Level 1 or Level 2 Access eAuthentication account. An eAuthentication account has an associated user ID and password which enables the electronic authentication of users. A user will then have access to authorized resources without needing to reauthenticate within the context of a single internet session. The user ID and password and permissions associated with an account are what authenticates and authorizes a user to access a requested USDA resource.

A customer **eAuthentication Level 1 Access webusers account** provides limited access to USDA Web site portals and applications that have minimal security requirements. Level 1 Access does not allow you to conduct official business transactions with the USDA via the Internet. A Level 1 Access account may be used to customize a web portal page, obtain general information about a specific USDA agency, and participate in public surveys for a USDA agency. A registrant can apply for a Level 1 Access account directly from the USDA eAuthentication Web site, located at www.eauth.egov.usda.gov. After accessing the

eAuthentication Web site the registrant must click on the *Create an account* tab located on the left-hand navigation bar and subsequently click on the *Level 1 Access* link located within the context of the web page. The registrant must then complete and submit the registration form. Once the Level 1 Access self-registration form is submitted, a Level 1 Access account is created in the eAuthentication system and an email is sent to the registrant confirming their registration for a Level 1 Access account. In order to activate the account the registrant must click on the *ACTIVATE MY ACCOUNT* link in the email message. The user is now able to provide their eAuthentication account credentials to access protected USDA resources requiring a Level 1 Access.

A customer **eAuthentication Level 2 Access webusers account** provides access to all the portals and applications that are covered by an account with Level 2 Access, and also provides the ability to conduct official electronic business transactions with the USDA via the Internet. A Level 2 account also enables customers to enter into a contract with the USDA and submit forms electronically via the Internet with a USDA agency. Similarly, a registrant can apply for an eAuthentication Level 2 Access account directly from the USDA eAuthentication web site. After the registrant clicks on the appropriate Level 2 Access links, completes and submits the Level 2 Access self-registration form, and responds to the confirmation email, a Level 1 Access account is created in the system. An activated Level 2 Access account is not provided until the registrant is identity proofed. The registrant must then present their government issued photo ID at their local USDA Service Center. The USDA Service Center employee, a trained local registration authority, confirms the registrant's identity and activates their Level 2 Access account. Approximately one hour after the Level 2 Access has been activated by the USDA Service Center employee, the registrant will have access to USDA applications and services that require an account with Level 2 Access.

Informational data that must be reported through the online self-registration form in order to obtain a Level 1 Access account are: User ID, Password, First Name, Last Name, Country Name, and Email address. Although not required, the registrant may also provide their Middle Name, and Zip Code. Due to the increased level of access to USDA applications, users must provide additional informational items to obtain a Level 2 Access account. in order to obtain a Level 2 Access account the registrant must also provide their: Home Address, City, State, Mother's Maiden Name, 4 digit PIN number, and Date of Birth, in addition to the information that must be provided to obtain a Level 1 Access account. The registrant also has the option to provide their Home Phone number or International Home Phone number (if applicable), and an Alternate Phone number or International Alternate Home Phone number (if applicable).

The online self-registration process to obtain an eAuthentication account is a one-time information collection process. The account information can be modified without the need of the user to re-register.

An eAuthentication account enables customers to access eAuthentication-protected USDA Web-based applications. These resources have been integrated with the eAuthentication Service to enable electronic authentication and authorization of users. Certain personal information collected through the online self-registration process is conditionally shared with USDA Agencies in order to integrate USDA resources with the eAuthentication service. Sensitive data such as Date of Birth, Mother's Maiden Name, Password, and other security related data is not shared. The eAuthentication Service ensures that shared data is transmitted to a system that has an approved and valid Certification and Accreditation (C&A) Authority to Operate (ATO) in effect. In addition, the eAuthentication Service ensures that shared data is securely managed by requiring a Privacy Impact Assessment (PIA) and Memorandum of Understanding (MOI) with the target system.

3. Use of information technology.

All technology used in the eAuthentication System is compliant with NIST Special Publication 800-63: *Electronic Authentication Guideline*. Users can obtain an eAuthentication Level 1 or Level 2 Access account solely through the online self-registration forms in the USDA eAuthentication Web site, located at www.eauth.egov.usda.gov. There is not a paper based form available to register for an eAuthentication account. Users must access the eAuthentication Web site and complete and submit the self-registration forms electronically over the Internet. There are separate online self-registration forms for a Level 1 and Level 2 Access account. The self-registration form for a Level 2 Access account requires additional user data due to the increased level of access. The self-registration forms can be access directly from the following links:

Level 1 Access -
https://eauth.sc.egov.usda.gov/eAuth/selfRegistration/selfRegLevel1Step1.jsp

Level 2 Access -
https://eauth.sc.egov.usda.gov/eAuth/selfRegistration/selfRegLevel2Step1.jsp

Each eAuthentication account contains an associated user ID and password that was created by the user. In addition, each account contains associated roles or permissions, given by administrators, which allow the user to access requested applications. The user ID and password and permissions associated with an account are what authenticates and authorizes a user to access a requested USDA resource.

The eAuthentication Service complies with the Government Paperwork Elimination Act (GPEA) by eliminating the need for traditional paper-based forms. In addition, eAuthentication provides full electronic reporting capabilities as required in the GPEA. However, obtaining an active Level 2 Access account electronically is not feasible since the higher level of access requires manual validation of a user's identity. Once the user is authenticated in-person by a trained local registration authority at a USDA Service Center it is recorded in the eAuthentication system which can then be accessed for auditing purposes.

4. Describe efforts to identify duplication.

USDA has built the eAuthentication Service with the elimination of duplication in mind. eAuthentication prevents users from creating and/or maintaining multiple online accounts with USDA. All eAuthentication accounts have a unique user ID. Once a registrant submits an account application the system automatically searches for pre-existing user IDs and prevents duplication of an account's key identifier. Not all USDA customers need an eAuthentication account, only those who are requesting access to USDA resources that are protected by eAuthentication. Therefore, the eAuthentication Service can not obtain customer information from other systems. There is also no alternate USDA enterprise service for authenticating and authorizing users electronically.

5. Methods used to minimize burden on small businesses or other small entities.

The reporting requirements in this information collection package will not affect small businesses. The online self-registration form is identical for all applicants irrespective to their volume or business. Therefore, no additional burden is being placed on businesses of any particular size.

6. Consequence if the information collection is not conducted or is conducted less frequently.

The information collected through the online eAuthentication self-registration form will only need to be collected once. If the information is not ever collected, the user must continue to conduct business with USDA through the existing paper-based processes.

7. Special Circumstances.

The information collected is consistent with provisions of the Paperwork Reduction Act of 1995 (PRA, 44 U.S.C. chapter 35), set forth in 5 CFR 1320.6.

8. Federal Register notice, summarization of comments, and consultation with persons outside the agency.

This section will be completed once the 60-day federal register notice has been published and 60 days have elapsed.

9. Explain any decision to provide any payment or gift to respondents.

The agency does not provide any payments or gifts to respondents for information collected through the USDA eAuthentication Web site.

10. Confidentiality provided to respondents.

All information collected will be treated as confidential in compliance with the Privacy Act and Freedom of Information Act.

11. Questions of a sensitive nature.

The information requested through the eAuthentication Web site is not considered of a sensitive nature (such as religious beliefs, sexual behavior and attitude, etc.).

12. Estimate of burden.

Refer to the attached burden grid for a breakdown of the burden estimate for the online eAuthentication account registration form.

USDA Agency customers can register for an eAuthentication Level 1 and Level 2 Access account. Registrants must submit a one-time online self-registration form and respond to a confirmation email to obtain an activated account. In order to obtain an active Level 2 Access account, the registrant's identity must be manually validated at a USDA Service Center.

The USDA eAuthentication Service has been operating since October 2003. From October 2003 – May 2005 there has been an average of 2,104 new Level 1 Access and 1,113 new Level 2 Access account registrations each month. During this time period the number of integrated USDA applications with eAuthentication has increased from 40 applications to over 110 applications. The eAuthentication Service estimates that there will be a similar rate of expected new registrations annually. Therefore, eAuthentication estimates that there will be 25,248 (2,104 registrants * 12 months) new Level 1 Access account registrations annually. Similarly, there will be an estimated 13,356 (1,113 registrants * 12 months) new Level 2 Access account registrations annually. Collectively, eAuthentication estimates 38,604 (25,248 Level 1 + 13,356 Level 2) new account registrations annually. There are no entries on the online form that requires any applicant to develop new information not already known by the applicant.

For a **Level 1 Access account** it is estimated to take 8 minutes (0.13 hours) to read, understand, and complete the online self-registration form. The estimated annual cost to the public is $30,096, which is based on the annual burden of 3,282 hours (25,248 responses * 0.13 hours) times an average hourly wage of $9.17 per customer. The average hourly wage is based on the mean hourly rate of Farming, Fishing, and Forestry Occupations in the Agriculture, Forestry, Fishing and

Hunting sector of the May 2004 National Industry-Specific Occupational Employment and Wage Estimates. This estimate is provided through the Bureau of Labor Statistics and can be directly accessed at http://www.bls.gov/oes/current/naics2_11.htm#b45-0000.

For a **Level 2 Access account** it is estimated to take 10 minutes (0.17 hours) to read, understand, and complete the online self-registration form. This amounts to an estimated annual cost to the public of $20,825, which is based on the annual burden of 2,271 hours (13,356 responses * 0.17 hours) times an hourly wage of $9.17 per customer. In addition, there is a cost associated with the travel time to the USDA Service Center for a customer's identity to be manually validated. The estimated time of travel for manual authentication is 1.0 hour. This amounts to an estimated annual cost to the public of $122,475, which is based on the annual burden of 13,356 hours (13,356 responses * 1.0 hour) times an hourly wage of $9.17 per customer. Collectively, there is an estimated annual cost to the public of $143,300 ($20,825 online form + $122,475 travel time).

13. Total annual cost burden to respondents.

The information collection and reporting burden does not impose any capital or start-up costs to respondents. The information requested is already available to respondents and there are no ongoing or follow-up reporting requirements that impose any costs but for the one-time collection.

14. Provide estimates of annualized cost to the Federal government.

The estimated cost to the Federal government is $100,821. This estimate is based on the cost of gathering, maintaining, retrieving, and disseminating the data. Despite fully supporting electronic information collection, additional time is sometimes needed to assist customers who are having difficulties. The estimated cost is based on requiring at least 10 minutes per response (38,604 annual responses) times the average of the GS-5 (step 5) through GS-7 (step 5) salary income of $32,598 per year or $15.67 per hour ($32,598/2080 hours per year).

15. Reasons for changes in burden.

This information collection request represents a new information collection to enable USDA customers to access protected USDA Web-based applications. Therefore, there are no changes in burden.

16. Outline plans for tabulation and publication.

The information collected is not planned for publication. It will only be used to provide the customer authorized access to applications.

17. Reasons display of expiration date for OMB approval of the information collection is inappropriate.

The USDA eAuthentication Service requests permission from OMB to not post the expiration date. The self-registration form will be used for a one-time registration process.

18. Exceptions to the certification statement identified in Item 19 of the OMB 83-I form.

There are no exceptions to the certification statement.